SecurITy 2002

Moderne Firewall Technologien in der Praxis

28. Januar 2002

René Pfeiffer

rene.pfeiffer@paradigma.net

Paradigma Unternehmensberatung GmbH

Wichtiger Hinweis:

Die Logfileauszüge dieses Vortrags enthalten zum Teil „echte" IP Adressen, die von Providern oder anderen Personen in Verwendung sind. Ich bitte diesen Umstand nicht als Anschuldigung zu verstehen oder daraus Maßnahmen oder Empfehlungen abzuleiten. Die Beispiel-Logs wurden bereits ausgewertet und in Einzelfällen wurden Schritte unternommen bzw. wurde der entsprechende Vorfall in Abstimmung mit der zutreffenden Security Policy behandelt. Ich bitte das Erscheinen der IP Adressen in keinster Weise als Bewertung, Kritik oder Anschuldigung zu sehen. Weiterhin bitte ich darum, diese IP Adressen keinen speziellen Untersuchungen wie Portscans, Security Audits oder ähnlichem ohne Zustimmung des Eigentümers zu unterziehen.

Zusätzliche Aufgaben einer Firewall

- **Network Intrusion Detection Systems (NIDS)**
  beobachten Pakete, die über das Netzwerk gesendet und empfangen wurden
  - Nachvollziehbarkeit von Vorfällen
  - Archivierung von Netzwerkaktivität
  - erfordert unter Umständen ein eigenes Netzwerk von Sonden
  - Logging alleine reicht nicht
    $\longrightarrow$ *Auswertung und Monitoring ist kritische Punkt*
- **System Integrity Verifiers (SIV)**
  überwachen kritische Bereiche eines laufenden Systems (Benutzerrechte, Binaries, Konfigurationen, etc.)
  - Systeme werden bei Installation mit Signatur versehen
  - „Fingerabdrucks" von Binaries durch Checksummen
  - Vergleich mit archivierten Signaturen
- **Log File Monitore (LFM)**
  durchsuchen Logfiles in regelmäßigen Abständen nach Anomalien
  - Koordinieren der Logs kann ein Problem werden
    $\longrightarrow$ *Time Stamps*
    $\longrightarrow$ *Zusammenführen der Logs von verschiedenen Orten*
  - Größe der Logs
    $\longrightarrow$ *Einsatz von Datenbanken*
    $\longrightarrow$ *Einsatz von Methoden des Data Minings*
- **Täuschen - Deceptions Systems**
  Vereiteln von Portscans, Ausgabe von Falschinformationen, Umschreiben der Mailheader

Sinn und Zweck zusätzlicher Aufgaben

- **Gegenprüfen der Paketfilter**
  - Portscanner und Packet Shaper als „Aggressoren"
  - „vergessene" Ports
  - Logging erzeugt Protokoll, welches den Zustand wiedergibt
- **Aufspüren von Attacken durch Kanäle, die die Firewall passieren**
- **Festhalten von fehlgeschlagenen Attacken**
  $\longrightarrow$ *Ermittlung von Trends bei den Eindringversuchen*
- **Sonden in interne Netzwerke**
  interne Netze bergen oft versteckte Gefahrenquellen
  - skriptfähige Mail User Agents
  - makrofähige Programme mit Schnittstellen zu anderer Software oder dem System
  - skriptfähige Web-Browser
  - eingeschleuste Trojaner & Viren

  LANs sind in der Regel nicht mehr als sichere Netzwerke zu betrachten.
- **Qualitätskontrolle des Sicherheitskonzepts**

Zustandsgesteuertes Paketfiltern unter Linux

- **Linux Netfilter ist zustandsgesteuert**
  verfügbar im Kern der 2.4.x Serie[1]
- **besseres ICMP Filtern**
  Filter kann ICMP Pakete zu bestehenden Verbindungen zuordnen
- **Connection Tracking**
  $\longrightarrow$ *Filtern von FTP und ähnlichen Protokollen*
  $\longrightarrow$ *Handhabung von Packetfragmenten*
  Zuordnen von geblockten Paketen

```
Sep 10 13:38:56 paladin kernel: IN= OUT=eth1
  SRC=26.100.46.116 DST=192.168.10.111 LEN=120 TOS=0x00
  PREC=0xC0 TTL=255 ID=18600 PROTO=ICMP TYPE=11 CODE=0
  [SRC=192.168.10.111 DST=213.47.27.79 LEN=92 TOS=0x00
  PREC=0x00 TTL=1 ID=26183 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=12800 ]
```

- **Filterregeln per User Account**
- **Rate Limiting**
  - Einstellen von Paketraten zum Schutz vor Paket■uten
  - Rate Limited Logging
- **modularer Aufbau mit Erweiterungen**
  - Filtern nach MAC Adresse
  - Sanity Checks mit verschiedenen Kriterien
  - Schnittstelle zu Paketfilter im User Space

[1] http://netfilter.samba.org/

Einsatzgebiet von Linux Paketfiltern

- **Router mit einem Subset von Filterregeln**
  - Netzwerkbereiche stellen verschiedene Anforderungen an Filter
  - Aufteilen der Filterfunktionen
  - begünstigt mehrstufige Verteidigung
- **interner Paketfilter zwischen LANs**
- **Paketfilter zwischen Standorten**
  - Einsatz von VPN Technologien (z.B. CIPE[2], IPsec[3])
  - On Demand Router (ADSL, ISDN, GSM)
- **Server Firewall**
  - Regeln können pro Benutzer Account eingestellt werden
  - netzwerkseitiges Beschränken von Applikationen
- **Kommerzielle Firewalls sind vorhanden**
  - Astaro Security Linux[4]
  - Mandrake Single Network Firewall 7.2[5]
  - SuSE Linux Firewall on CD[6]

[2] http://sites.inka.de/~W1011/devel/cipe.html
[3] http://www.freeswan.org/
[4] http://www.astaro.com/
[5] http://www.mandrakesoft.com/products/snf
[6] http://www.suse.de/de/products/suse_business/firewall/index.html

Einsatzgebiet von Linux als Content Filter
Content Filtering mit Squid Proxy

- **Squid[7] ist ein Web & Reverse Proxy**
  - Web Proxy für Browser als Clients
  - Reverse Proxy vor Web Servern
    - Load Balancer
    - Entlastung des Web Servers bei statischem Content
- **Koppelung mehrerer Squids als Parent/Child Cluster**
- **Benutzung von externen Programmen als URL Filter**
  - URL Request wird vom Squid nach Prüfung der ACLs angenommen
  - URL wird an ein externes Programm weitergegeben
  - externes Programm kann URL beliebig modifizieren
  - Squid holt tatsächlich die URL, die der Filter zurückgibt

  Einsatz zum Schutz von Web Servern

[7] http://www.squid-cache.org/

Squid als Reverse Proxy

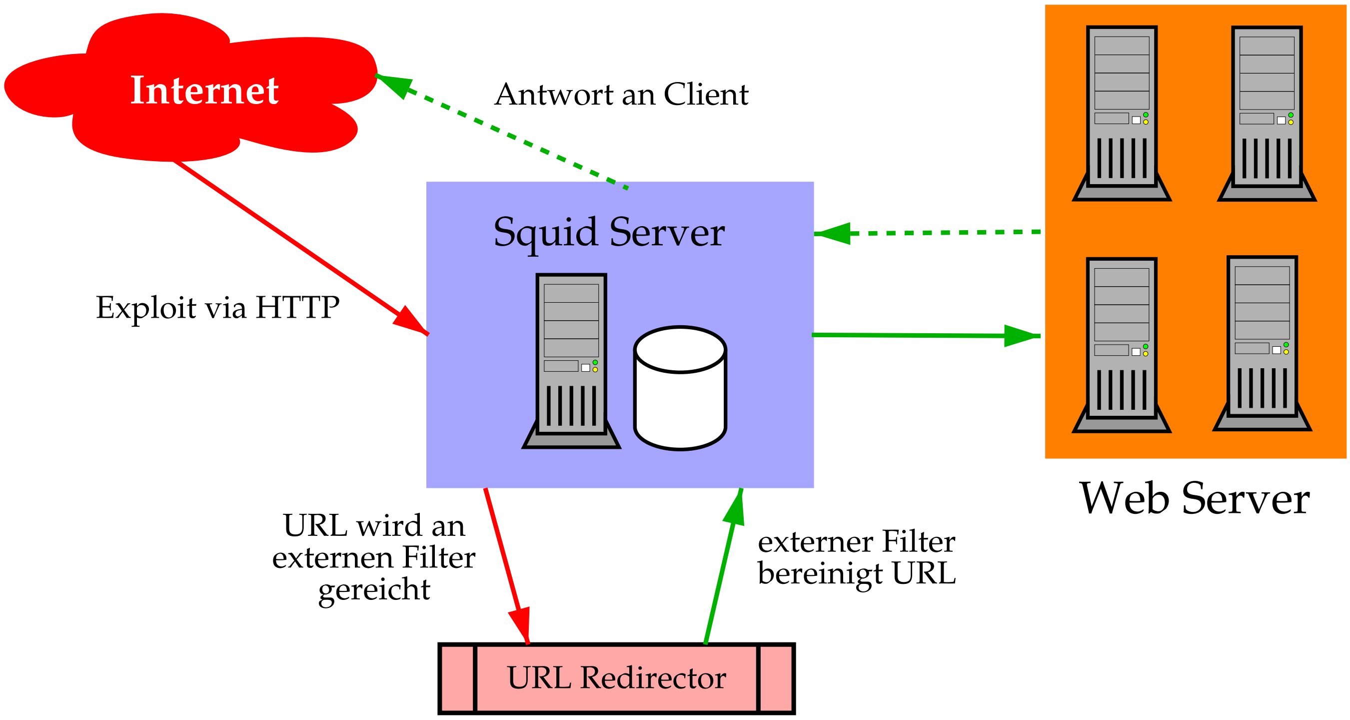


Abbildung 1: Ein Squid als Reverse Proxy mit URL Filtern vor einer Reihe von Web Servern. Das externe Filterprogramm am Squid prüft URLs auf Attacken und leitet diese um bzw. blockt sie.

Personal Firewalls

- **Personal Firewalls treten in die Fußstapfen der Anti-Virus-Software**
- **Konfiguration geschieht oftmals „vollautomagisch"**
  - fehlende Erfahrung beim Einsatz
  - fehlende Expertise beim Prüfen der Wirksamkeit
  - „light", „medium" oder „high" reicht nicht als Sicherheitsstufe
- **fehlende Trennung zwischen Schutzmaßnahme und Ziel**
  - Systemkompromittierung kann Filter unwirksam machen
  - Personal Firewall kann (un)absichtlich deaktiviert werden
- **Personal Firewalls haben psychologische Nebenwirkungen**
  - Erzeugen eines Sicherheitsgefühls durch bloßes Vorhandensein
  - sorgloseres Verwenden von fehleranfälliger Software
    $\longrightarrow$ *Personal Firewalls können damit Gefahren noch steigern*
- **Personal Firewalls gefährden VPNs**
  $\longrightarrow$ *erster Anti-Personal-Firewall Wurm wird durchschlagenden Erfolg haben*
- **Personal Firewalls sind kleiner Baustein eines Sicherheitskonzepts**

Network Intrusion Detection mit Snort

Die Fähigkeiten von Snort[8] umfassen

- **Real-Time Traffic Analyse**
- **Analyse von aufgezeichnetem Netzwerkverkehr**
- **Schreiben von Log-Daten in externe SQL Datenbank**
  normaler Betriebsmodus arbeitet mit Logs im Dateisystem
- **frei programmierbar durch Rule Sets**
  $\longrightarrow$ *beliebige Definition von Alerts*
  $\longrightarrow$ *Konfigurieren von automatischen Benachrichtigungen*
- **Flexible Response Option**
  Snort kann auf bestimmte Pakete mit einer Reihe von Antworten reagieren
- **Schnelligkeit**
  - Entkoppeln von Detektieren und Auswerten
  - Erfassen von 100 Mbit/s Link mit 80 Mbit/s

  Es gibt noch weitere Anstrengungen die Rate zu verbessern und schnellere Netzwerke zu beobachten.
- **Stealth Modus**
  Snort benötigt keinen TCP/IP Stack auf dem System

[8] http://www.snort.org/

Snort Filterregeln

- **Grundfunktionen** `alert / log / pass`
- unterstützt derzeit TCP, UDP & ICMP
  In Zukunft geplant: ARP, IGRP, GRE, OSPF, RIP, IPX
- **Snort kann die folgenden Paketinformationen testen**
  - `TTL` - Wert des IP Pakets
  - `ID` - IP Header Fragment ID
  - `DSIZE` - Datenlänge des IP Pakets
  - `Content` - bestimmter Inhalt in den Daten des IP Pakets (Pattern Matching)
  - `Flags` - TCP Flags
  - `SEQ` - TCP Sequenznummern
  - `ACK` - TCP ACK-Nummer
  - `Session` - beobachtet einzelne Sessions (Telnet, rlogin, FTP, HTTP)
  - `IType` - ICMP Typ
  - `ICode` - ICMP Code
  - `ICMP_Id` - ICMP Echo ID
  - `ICMP_Seq` - ICMP Echo Sequenznummer
  - `IPoption` - IP Options
    - rr - Record Route
    - eol - End of list
    - nop - No op
    - ts - Time Stamp
    - sec - IP security option
    - lsrr - Loose source routing
    - ssrr - Strict source routing
    - satid - Stream identifier
  - `RPC` - RPC Service/Applikations Aufrufe
- **Flexible Response -** `resp`
  Snort kann eine sich aufbauende Verbindung trennen

Snort Flexible Response

- **Senden von TCP-RST** an Empfänger, Sender oder beide
- **Senden von ICMP Nachrichten an den Sender**
  - ICMP Network Unreachable
  - ICMP Host Unreachable
  - ICMP Port Unreachable
- **Gegenmaßnahmen mit Checkpoint Firewall-1 über Snortsam**[9]
  - Liste von IPs, die nicht geblockt werden sollen
  - Kontrolle über Zeitintervalle
  - Rollback Support zur Aufhebung von Blocks
  - verschlüsselte Two-Fish Kommunikation zwischen Snortsam und Firewall-1
  - Plugin-Möglichkeit für andere Firewalls

Damit ist es möglich auf bestimmte Kriterien und Datenpakete zu reagieren.

[9] http://www.snortsam.net/

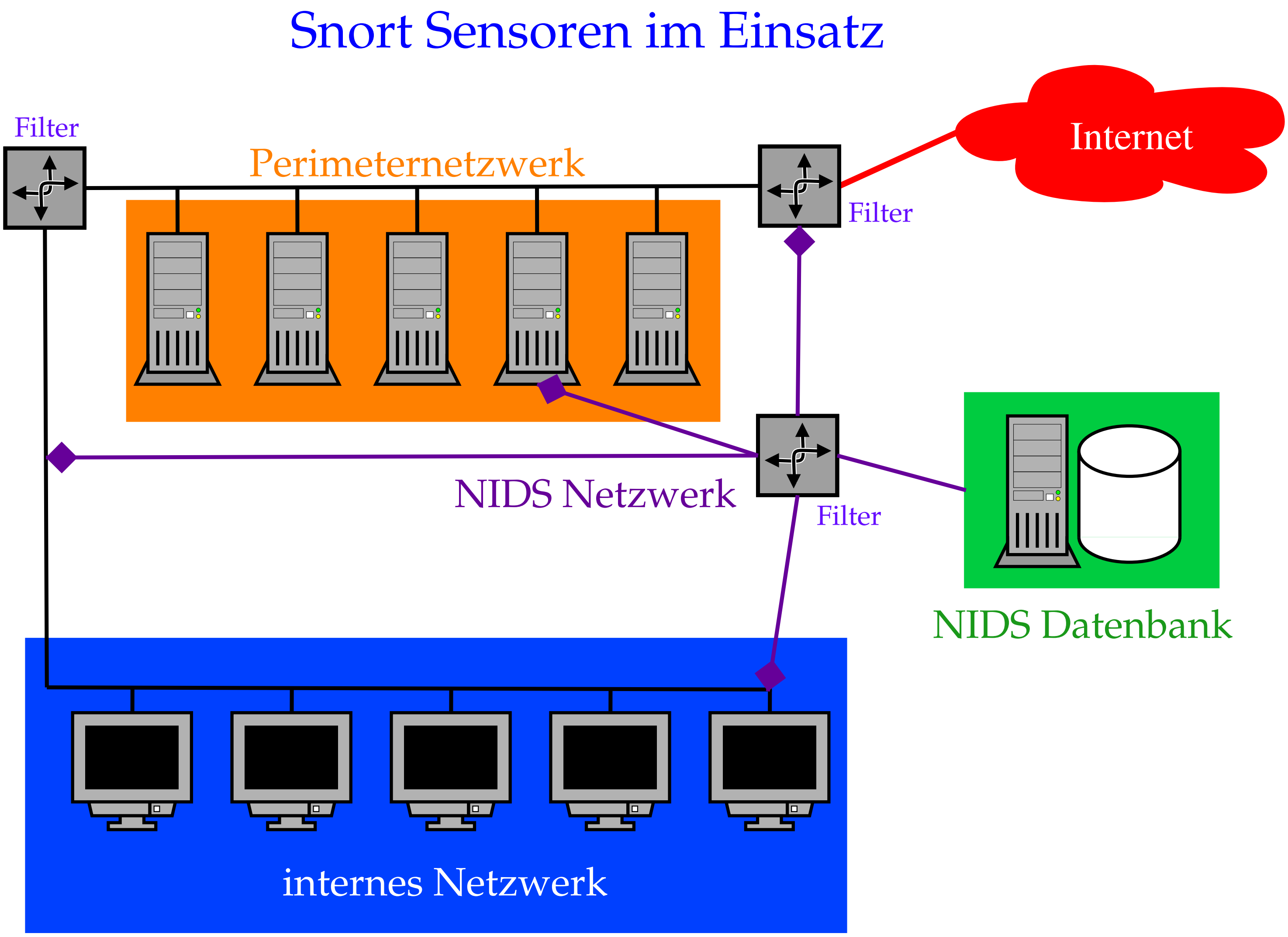


Abbildung 2: Schematischer Einsatz von Snort Sensoren in einem Netzwerk. Man kann Sensoren auf Paketfiltern, Servern oder auf speziellen Logservern unterbringen. Der sinnvollste Einsatz geschieht auf einer eigenen Maschine, die ausgewählten Netzwerkverkehr über einen dafür abgestellten Port an einem Switch erhält.

Methoden zur Netzwerküberwachung

- **Einsetzen von HUBs in Segmente**
  - *leicht zu implementieren, keine besondere Konfiguration*
  - *Netzkollisionen steigen, Performanceverlust*
- **Switch Port Analyzer (SPAN) Port**
  - *keine weitere Hardware nötig, Infrastruktur bleibt unverändert*
  - *begrenzte Anzahl von Ports pro Switch, NIDS nur passiv*
- **Network Taps**
  - *kein Performanceverlust, keine Störung am Netzwerk*
  - *NIDS muß im Stealth Mode arbeiten, Kostenfaktoren*

Generell hängt der Einsatz von IDS von der Netzwerkstruktur ab und muß angepaßt werden.

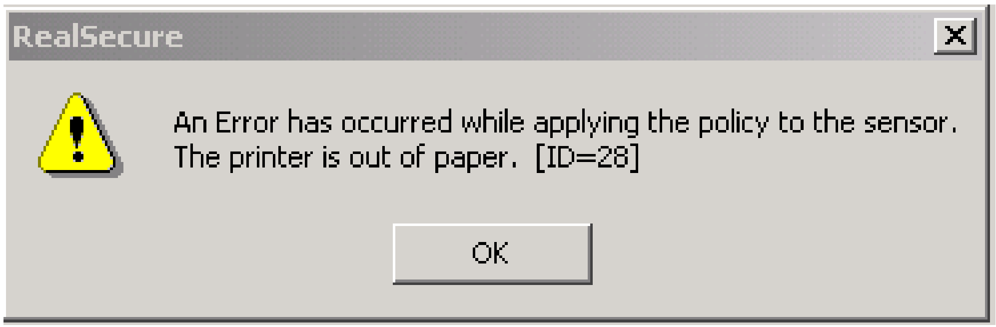
NIDS Zonen

- **unsichere Netzwerke**
  - hohe Rate von Alarmen und Fehlalarmen
  - High Risk Zone
  - Sensitivität von NIDS muß gering sein
- **Perimeternetzwerk**
  - mittlere Rate von Alarmen und Fehlalarmen
  - Netzwerkverkehr ist vorgefiltert
  - Sensitivität von NIDS muß mit Umgebung abgestimmt sein
- **lokale/vertrauenswürdige Netzwerke**
  - geringe bis mittlere Rate von Alarmen und Fehlalarmen
  - in der Regel keine Paketfilter zwischen den Clients
  - NIDS kann nach eingeschleusten Risiken schauen
  - höchster Anspruch an Performance

Gleichgewicht der Kräfte

- **technische Möglichkeiten sind extrem vielfältig**
  ⟶ *Gefahr von übermäßig komplexen Maßnahmen*
  ⟶ *Propagierung von Universalmedikamenten*

- **„Domino Theorie"**
  - Firewall- und IDS-Implementationen können eine Kette von Abhängigkeiten bilden
  - Ausfälle in Teilbereichen können IDS daher unbrauchbar machen



  - Ausfallsicherheit kann Aufwand für Systemadministration erhöhen

- **Mächtigkeit von Paketfiltern bringt neue Risiken**
  - Paketfilter besteht aus Software, die Bugs haben kann
  - Paketfilter sollten robust implementiert sein
  - „Feature Freeze" ist auch für Systemadministration sinnvoll

Attacken gegen NIDS Implementationen

- **Sensor mit Paketflut blenden**
  - IP Pakete mit gefälschten Quelladressen
  - fragmentierte Pakete
  - Versuch den Sensor durch Überlastung auszuschalten (CPU, Storage, Alarmrate)
  - Mischen von Attacken und Paketflut zur Täuschung
- **langsame Proben und Portscans**
  - Proben können sich über Tage und Wochen hinziehen
  - Detektierung durch manuelle Auswertung unmöglich
- **koordinierte Attacken von verschiedenen Ausgangspunkten**
- **wechselnde Muster bei Proben und Attacken**
  $\longrightarrow$ *manche Attackvektoren erlauben Variationen*
  $\longrightarrow$ *gute Definition und Wartung von Signaturen notwendig*
- **Verwenden von nicht-standard Ports**
  oft wird ein Protokoll nur nach Portnummer identifiziert

Quelle: `http://www.robertgraham.com/pubs/network-intrusion-detection.html`

Auswerten der IDS Daten

- **IDS generieren sehr viele Daten**
- **datenbankgestützte Auswertung für ernsthafte Analyse erforderlich**
  - Einsatz von Data Mining Methoden
  - Erkennen von Mustern und Anomalien
- **Korrelation der IDS Daten mit anderen Logs**
  - Systemlogs (z.B. *syslogd*)
  - Maillogs
  - Web- und FTP-Server Logs
  - Logindaten (z.B. SSH, RADIUS, VPN Connects)
  - Disk I/O, Netzwerklast, CPU Last

  Korrelation erfordert Zeitsynchronisation aller Sonden!
- **Human Intelligence ist gleichermaßen erforderlich**

Manuelle Auswertung - ACID

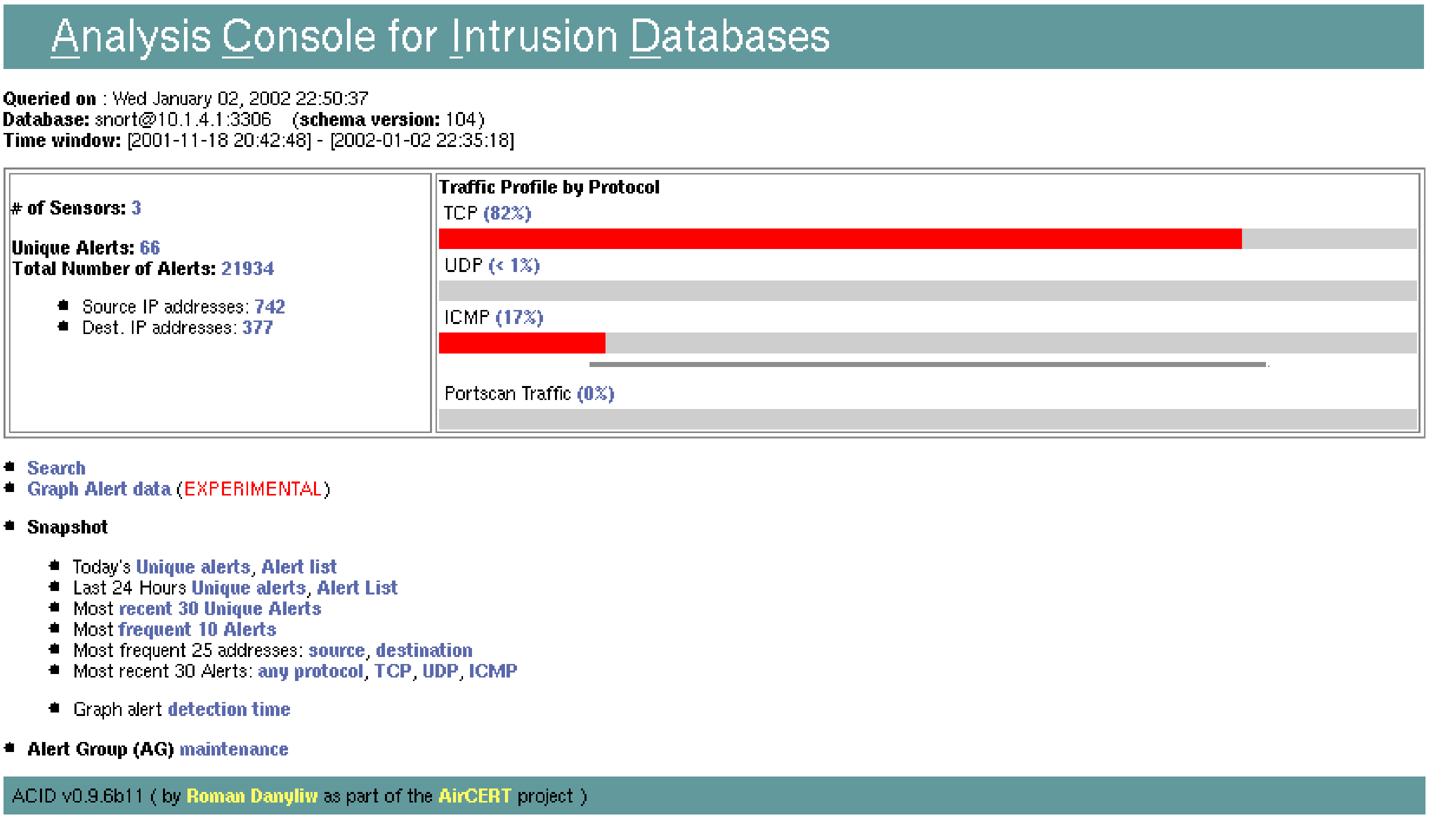
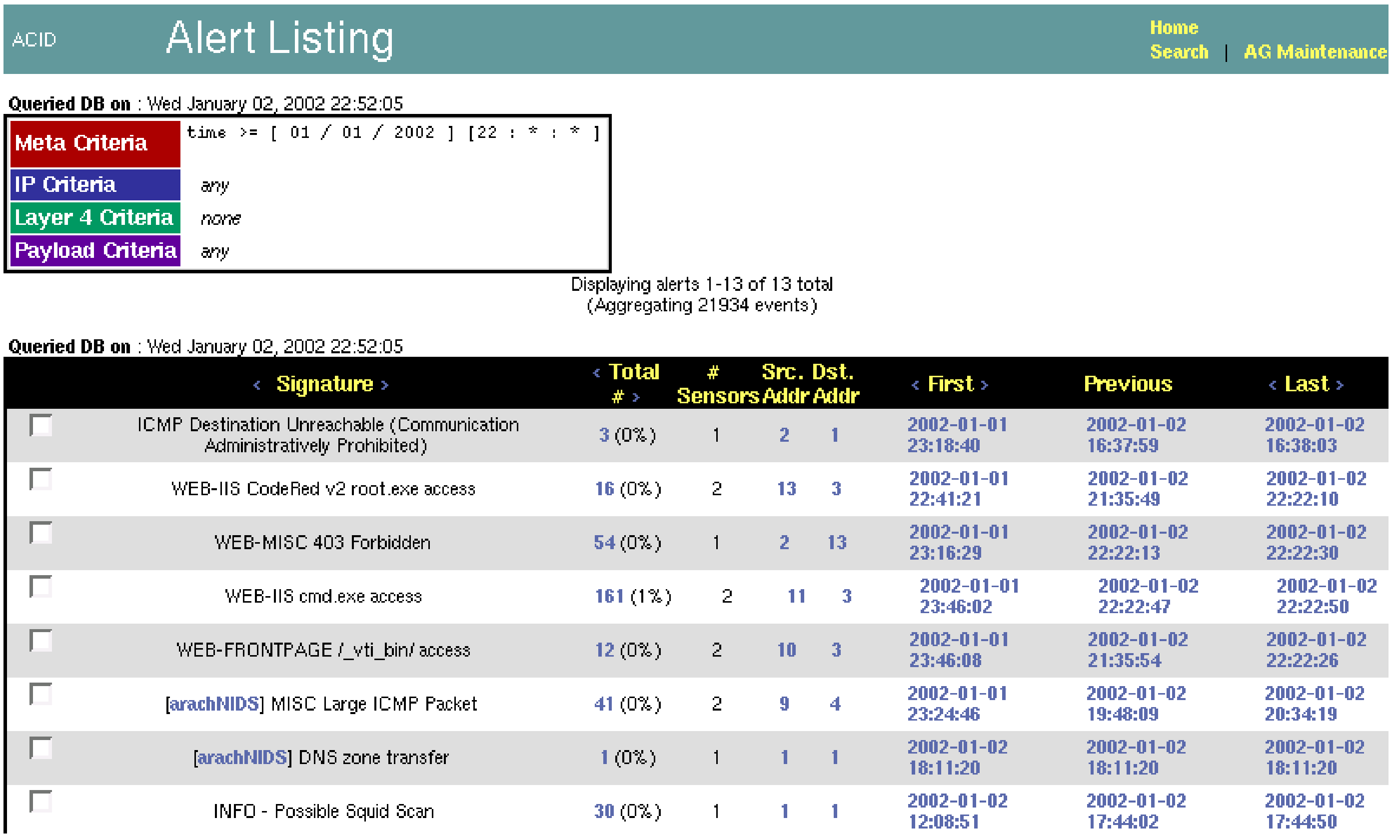


Abbildung 3: Die Abbildung zeigt die Analysis Console for Intrusion Databases (ACID). ACID besteht aus einer PHP4 Applikation, die Snort Ereignisse aus einer SQL Datenbank darstellen und bearbeiten kann. (`http://www.cert.org/kb/aircert/`)

Manuelle Auswertung - ACID Details



ACID Alert Listing

Home
Search | AG Maintenance

Queried DB on : Wed January 02, 2002 22:52:05

Meta Criteria	time >= [01 / 01 / 2002] [22 : * : *]
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Displaying alerts 1-13 of 13 total
(Aggregating 21934 events)

Queried DB on : Wed January 02, 2002 22:52:05

	< Signature >	< Total # >	# Sensors	Src. Addr	Dst. Addr	< First >	Previous	< Last >
☐	ICMP Destination Unreachable (Communication Administratively Prohibited)	3 (0%)	1	2	1	2002-01-01 23:18:40	2002-01-02 16:37:59	2002-01-02 16:38:03
☐	WEB-IIS CodeRed v2 root.exe access	16 (0%)	2	13	3	2002-01-01 22:41:21	2002-01-02 21:35:49	2002-01-02 22:22:10
☐	WEB-MISC 403 Forbidden	54 (0%)	1	2	13	2002-01-01 23:16:29	2002-01-02 22:22:13	2002-01-02 22:22:30
☐	WEB-IIS cmd.exe access	161 (1%)	2	11	3	2002-01-01 23:46:02	2002-01-02 22:22:47	2002-01-02 22:22:50
☐	WEB-FRONTPAGE /_vti_bin/ access	12 (0%)	2	10	3	2002-01-01 23:46:08	2002-01-02 21:35:54	2002-01-02 22:22:26
☐	[arachNIDS] MISC Large ICMP Packet	41 (0%)	2	9	4	2002-01-01 23:24:46	2002-01-02 19:48:09	2002-01-02 20:34:19
☐	[arachNIDS] DNS zone transfer	1 (0%)	1	1	1	2002-01-02 18:11:20	2002-01-02 18:11:20	2002-01-02 18:11:20
☐	INFO - Possible Squid Scan	30 (0%)	1	1	1	2002-01-02 12:08:51	2002-01-02 17:44:02	2002-01-02 17:44:50

Abbildung 4: Ereignisse der letzten 24 Stunden im Überblick.
(`http://www.cert.org/kb/aircert/`)

Mehrstufige Auswertung

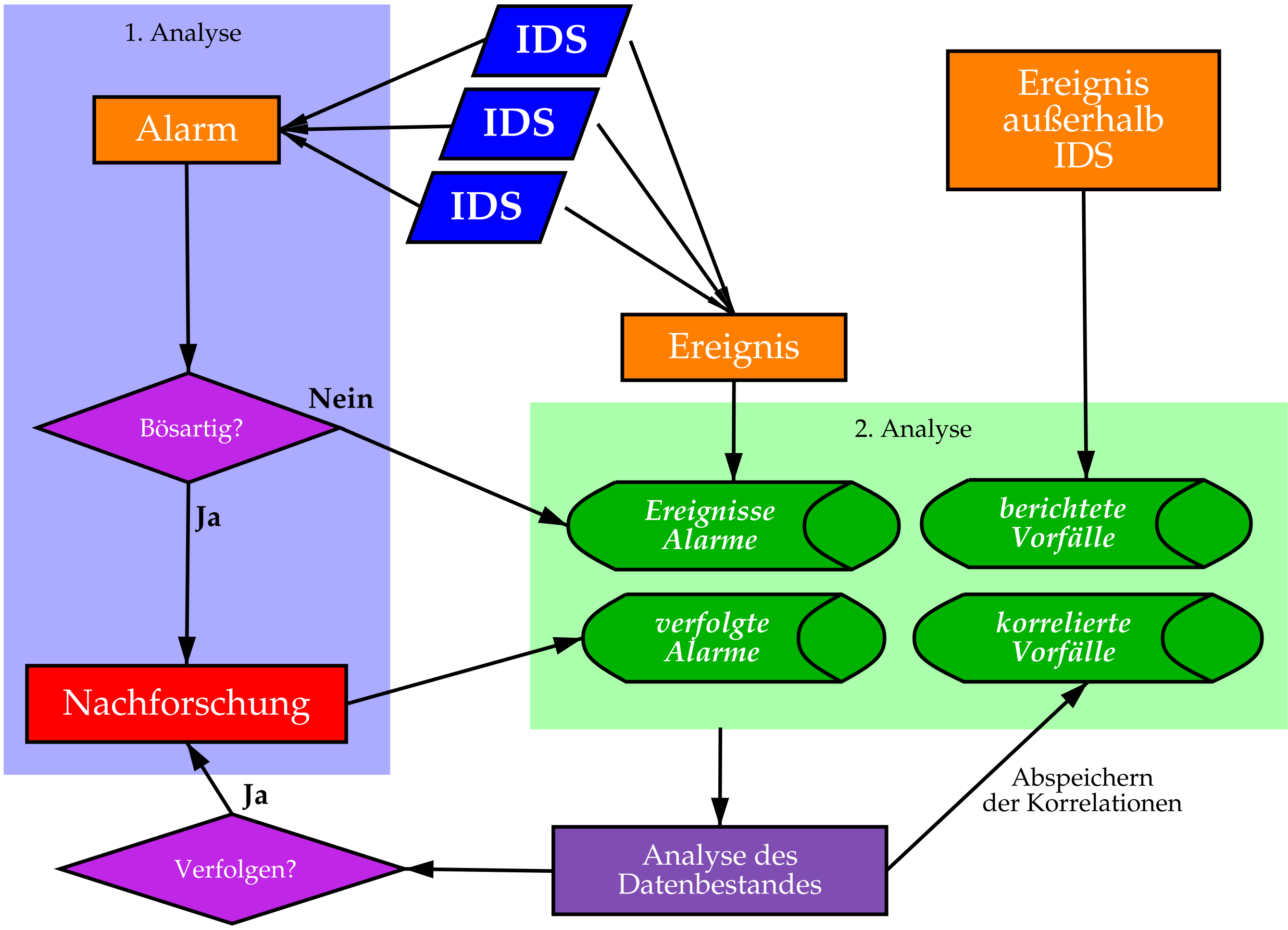


Abbildung 5: Die Abbildung zeigt die mehrstufige Auswertung von IDS Daten. In der ersten Stufe wird unmittelbar auf einen Alarm reagiert. Die Daten werden in Datenbanken gesammelt und durch weitere Prozesse analysiert. Dadurch können sich weitere Alarme ergeben, die behandelt werden müssen. (`http://www.securityfocus.com/infocus/1201`)

Strategische und taktische Updates

- **Stichwort Proaktive Sicherheit**
  Wartungskonzept ist mit Backupkonzept gleichwertig
- **Distributionsserver zum Verteilen der Updates**
  - kontrolliertes Sammeln aller relevanten Patches und Updates
  - Generieren von eigenen Updates (RPM[10], UNIX `tar`)
  - kryptographisches Prüfen der Updates
    ⟶ *Distributoren signieren ihre Updates*
- **freie Verfügbarkeit von Security Advisories wichtig**
  - Zensur wird niemals gute Systemadministration überflüssig machen
  - Systemadministration kann vor den Herstellern Workarounds finden
  - schnelles Reagieren ist der Schlüssel zum sicheren Netzwerk

[10] http://www.rpm.org/

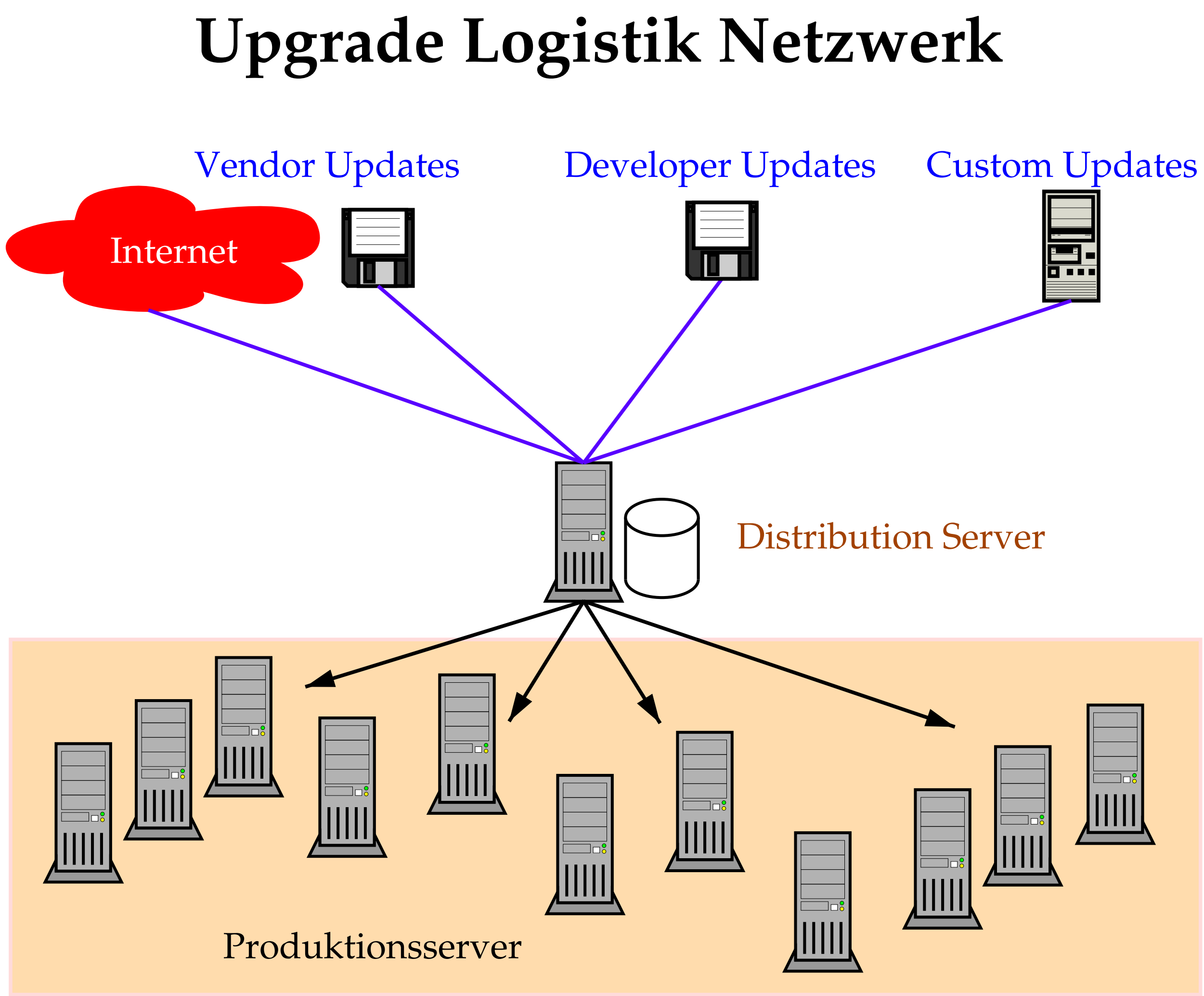


Abbildung 6: Das Diagramm zeigt eine schematische Darstellung eines Upgrade Logistik Netzwerks. Solche Anordnungen sind ab mittleren Netzwerken sehr sinnvoll.

PARADIGMA

Vielen Dank!